WHAT IS CLAIMED IS:

1. A method, under the PKI environment, of the key generation and escrow, comprising the steps of:

(a) having the user generate a password and register a password verifier of the user in a key management authority;

(b) having the user generate a pair of private/public keys;

(c) having the user encrypt his own private key with his own password (i.e. $C = E_{PWD}(PRI$, where PWD is user's password and PRI is user's private key)

(d) having the user generate a key recovery block through encryption of the encrypted private key C with a public key of a key recovery agents.

(e) sending user's key recovery block and public key to the key management authority; and

(f) having the key management authority store the key recovery block, or divide it into several shares, followed by storing the shares separately.

2. A method, under the PKI environment, of the key generation and escrow, comprising the steps of:

(a) having the user generate a password and register a password verifier of the user in a key management authority;

(b) having the user generate a pair of private/public keys;

(c) having the user encrypt his own private key with his own password (i.e. $C = E_{PWD}$ (PRI , where PWD is user's password and PRI is user's private key)

(d) having the user generate a key recovery block through encryption of the encrypted private key C with a public key of a key recovery agents.

(e) checking the validity of the key recovery block;

(f) sending user's validated key recovery block and public key to the key management authority;

(g) having the key management authority store the key recovery block, or divide it into several shares, followed by storing the shares separately.

3. The method as described in Claim 2 wherein said step (c) is skipped and said step of (d) comprises a step of generating a key recovery block through the encryption of said user's private key with a public key of a key recovery

agent by said user.

4. A method, under the PKI environment, of the key generation and escrow, comprising the steps of:

(a) having the user register his password in a key management authority(KMA);

(b) having the KMA generate a pair of private/public keys for the user;

(c) having the KMA encrypt the user's private key with the registered password of the user (i.e. $C = E_{PWD}(PRI)$, where PWD : user's password, PRI : user's private key);

(d) having the KMA generate a key recovery block(KRB) through the encryption of said encrypted private key C with a public key of a key recovery agents (KRAs); and

(e) having the KMA either to store the KRB, or to divide the KRB into several shares, followed by separately storing said shares.

5. A method, under the PKI environment, of the key recovery, comprising the steps of:

(a) having a key management authority (KRA) construct a key recovery block (KRB) for the corresponding user upon the request for the key recovery;

(b) having the KMA to blind the

constructed key recovery block by employing a blind factor of said key management authority's own so that any KRA is not able to see said constructed key recovery block;

(c) having the KMA to send the blinded key recovery block along with a request for the key recovery to KRAs;

(d) having each KRA perform a decryption of the message received by employing a private key of its own;

(e) having each KRA send the decrypted message processed at step (d) to said key management authority; and

(f) having the KMA recover a encrypted private key C of said user by employing the message received from each key recovery agent and said blind factor of its own.

6. The method as described in Claim 5 wherein said request for the key recovery at step (a) is the request either from said user or from the court.

7. The method as described in Claim 5 wherein less than all of shares of the corresponding user's key recovery block are required to construct the key recovery block.

8. The method as described in Claim5 wherein less than all of the messages received from key recovery agents are required to recover the encrypted private key for the corresponding user.

9. The method as described in Claim5 further includes a step of having a key management authority send said recovered C to the key recovery requestor using the password-based private key downloading protocol.

10. The method as described in Claim5 wherein a key management authority or a trusted entity recovers the user's private key for encryption from C by mounting a dictionary attack.

11. The method as described in Claim 5 wherein a key management authority or a trusted entity recovers the user's private key for encryption with the user's registered passwords.

12. A key escrow system for the PKI environment comprising:

a user who generates his own password, registers his own password verifier in a key management authority (KMA), generates a pair of private/public key pairs (PRI, PUB), encrypts his private key with said password ($C = E_{PWD}(PRI)$),

and generates a key recovery block (KRB) through encrypting C with a public key of key recovery agents (KRAs)

a KMA that stores either said KRB or the divided shares of said KRB in a distributed manner, constructs said KRB from the divided shares at a key recovery phase, sends to KRAs a request for the key recovery along with a blinded KRB which is a multiplication of said KRB with a blind factor in order not to disclose said KRB to any of said KRAs, and recovers C with received messages from said KRAs and with said blind factor; and

KRAs that decrypt message sent from said KMA with the private key of their owns.

13. The key escrow system as described in Claim 12 wherein said KRB generated by said user is checked for the validity.

14. A key escrow system for PKI environment comprising:

a user who registers his password (PWD) in a key management authority (KMA), comprising:

a KMA that generates a pair of private/public keys (PRI, PUB) for said user, encrypts said user's private key with said user's registered password ($C = E_{PWD}(PRI)$,

generates a key recovery block (KRB) through encrypting C with the public key of the key recovery agents (KRAs), stores said KRB or the divided shares of said KRB in a distributed manner, reconstructs said KRB out of said divided shares upon the request for recovery, sends to KRAs a request for recovery along with a blinded KRB which is a multiplication of said KRB with a blind factor in order not to disclose said KRB to any of said KRAs, and recovers C with received messages for said KRAs and with said blind factor; and

KRAs that decrypt messages sent from said KMA with private keys of their own.

15. The key escrow system as described in Claim 12 or Claim 14 wherein less than all of shares of the corresponding user's key recovery block are required to construct the key recovery block.

16. The key escrow system as described in Claim 12 or Claim 14 wherein less than all of the messages received from key recovery agents are required to recover the encrypted private key for the corresponding user.